Fermilab Top-Level CA Certificate Policy
and Certification Practices Statement

8 August 2003

# 1. INTRODUCTION

## 1.1. Overview

This document follows the structure suggested in RFC 2527.

The public key infrastructure of Fermilab comprises three certificate authorities: the KCA, the Service CA and the Top-Level CA. This document specifies the policies and practices under which the Top-Level CA is operated.

## 1.2. Identification

Document title
Fermilab Top-Level CA Certificate Policy and Certification Practices Statement

Document version
Revision: 1.3

Document date
Date: 2003/08/08 22:58:31 UTC

OID 1.3.6.1.4.1.14147.1.5.1

## 1.3. Community and Applicability

### 1.3.1. Certification Authorities

The Fermilab Top-Level CA certifies only other CAs located at and operated by Fermilab.

### 1.3.2. Registration Authorities

No Registration Authorities are involved in the operation of the Fermilab Top-Level CA.

### 1.3.3. End Entities

The Fermilab Top-Level CA does not issue certificate to end-entities of any kind.

### 1.3.4. Applicability

Keys certified by the Fermilab Top-Level CA are intended and suitable only for the operation of subordinate CAs and for no other purpose. Such keys are valid for Digital Signature, Certificate Signing, and CRL Signing.

## 1.4. Contact Details

The Fermilab Top-Level CA is established, maintained and operated by the Fermilab Computer Security Team. The contact person for this document is the Fermilab Computer Security Coordinator.

Matt Crawford
Fermilab MS-369
PO Box 500
Batavia IL 60510
USA

Phone: +1 630 840 3461
Fax: +1 630 840 6345
Email: nightwatch@fnal.gov

# 2. GENERAL PROVISIONS

## 2.1. Obligations

### 2.1.1. CA Obligations

The Fermilab Top-Level CA will

* Accept certificate and revocation requests only from those members of the Fermilab Computer Security Team involved in operating Fermilab CAs.

* Publish issued certificates in a well-known location.

* Publish CRLs in a timely manner and in well-known locations.

### 2.1.2. RA Obligations

No RAs are involved.

### 2.1.3. Subscriber Obligations

No subscribers are involved.

### 2.1.4. Relying Party Obligations

Relying parties must

* Be cognizant of the provisions of this document.

* Verify any self-signed certificates to their own satisfaction using out-of-band means.

* Accept responsibility for checking any relevant CRLs before accepting the validity of a certificate.

* Observe restrictions on private key and certificate use.

### 2.1.5. Repository Obligations

Certificate and Revocation information is maintained on-line with an intended availability of 100%, but the repository is operated on a best-effort basis.

## 2.2. Liability

The Fermilab Top-Level CA is operated substantially in accordance with Fermilab's own risk analysis. No liability, explicit or implicit, is accepted.

The Fermilab Top-Level CA and its agents make no guarantee about the security or suitability of a service that is identified by a Fermilab certificate. The certification service is run with a reasonable level of security, but it is provided on a best effort basis. It does not warrant its procedures and it will take no responsibility for problems arising from its operation, or for the use made of the certificates it provides.

The Fermilab Top-Level CA denies any financial or any other kind of responsibility for damages or impairments resulting from its operation.

## 2.3. Financial Responsibility

No financial responsibility is accepted.

## 2.4. Interpretation and Enforcement

This policy is subordinate to all applicable U.S. government laws, as well as Department of Energy (DOE) orders.

## 2.5. Fees

No fees are charged.

### 2.6. Publication and Repositories

#### 2.6.1. Publication of CA information

The Fermilab Top-Level CA will operate an online repository that contains

* Fermilab CA certificates.
* A Certificate Revocation List.
* A copy of this policy.
* Other information deemed relevant to the Fermilab PKI.

#### 2.6.2. Frequency of Publication

* CA certificates will be published in the repository as soon as they are issued.
* CRLs will be published as soon as they are updated, or monthly if there are no changes.
* Fermilab PKI documents will be published in the repository as they are approved.

#### 2.6.3. Access Controls

The CA publication repository is always available, outside of maintenance times and unforeseen failures. The Fermilab Top-Level CA imposes no restrictions on the accessibility of published information.

#### 2.6.4. Repository Location

http://computing.fnal.gov/security/pki/

### 2.7. Compliance Audit

The Fermilab Top-Level CA will be included in Fermilab's regular computer security self-assessment and peer review process but will not be specifically audited by an outside party. Certifying, cross-certifying, and relying organizations may request a review of Fermilab PKI operation.

### 2.8. Confidentiality Policy

The Fermilab Top-Level CA considers the contents of CRLs and certificates to be public information. The Fermilab Top-Level CA does not obtain or store copies of private information about individuals.

### 2.9. Intellectual Property Rights

The Fermilab Top-Level CA asserts no ownership rights in certificates issued to subscribers. No claims are made regarding documents produced by the CA other than as specified in Fermilab's operating contract with the U.S. Department of Energy. Acknowledgment is hereby given to the DOE Science Grid and to the CERN Certification Authority for inspiration of parts of this document.

## 3. IDENTIFICATION AND AUTHENTICATION

### 3.1. Initial Registration

#### 3.1.1. Types of Names

Subject distinguished names are X.500 names, with components varying depending on the type of certificate.

All subject distinguished names in certificates issued by the Fermilab Top-Level CA begin with ''DC=gov, DC=fnal, O=Fermilab, OU=Certificate Authorities''.

#### 3.1.2. Name Meanings and Interpretation

The CN component of the subject name in issued certificates designates the role of the CA to which they are issued.

#### 3.1.3. Name Uniqueness

Each subject name certified by the Fermilab Top-Level CA will be unique.

#### 3.1.4. Name Disputes

The Fermilab Top-Level CA will resolve disputes as it sees fit.

#### 3.1.5. Method to Prove Possession of Private Key

No stipulation.

#### 3.1.6. Authentication of Organizational Identity

The Fermilab Top-Level CA certifies only CAs operated by the same organization as itself.

#### 3.1.7. Authentication of Individual Identity

The Fermilab Top-Level CA will not issue certificates to individuals.

### 3.2. Routine Rekeying

Routine rekeying follows the same rules as an initial registration.

#### 3.2.1. Rekey after Revocation

Rekeying after revocation follows the same rules as an initial registration.

### 3.3. Revocation Requests

Certificates will be revoked only at the instigation of the Fermilab Computer Security Team.

## 4. OPERATIONAL REQUIREMENTS

### 4.1. Certificate Application

CA certificate requests must be initiated by the Fermilab Computer Security Team.

### 4.2. Certificate Issuance

CA certificates are issued only to the Fermilab Computer Security Team.

### 4.3. Certificate Acceptance

No stipulation.

### 4.4. Certificate Suspension and Revocation

Certificates issued by the Fermilab Top-Level CA will not be suspended.

#### 4.4.1. Circumstances for Revocation

Certificates will be revoked promptly if the associated private key is known to be lost or reasonably suspected to be compromised.

#### 4.4.2. Requesting Revocation

Only members of the Fermilab Computer Security Team may request revocation.

#### 4.4.3. Verifying Revocation Requests.

No stipulation.

#### 4.4.4. CRL Issuance Frequency

CRLs for the Service and Top-Level CAs will be issued upon any change in their contents, or monthly if there are no changes. New CRLs will be published at least seven days before the expiration of the last previously-published CRL.

#### 4.4.5. Online Revocation/Status Checking Availability

The most recent CRL will be available online.

#### 4.4.6. Revocation/Status Checking Requirements

Relying parties are advised to obtain and consult a valid CRL.

### 4.5. Security Audit Procedures

No stipulation.

### 4.6. Records Archival

No stipulation.

### 4.7. Key Changeover

The community of known relying parties will be notified of any new CA public key and it may then be obtained in the same manner as the previous CA certificates.

### 4.8. Compromise and Disaster Recovery

Compromise of the Top-Level CA would mean the exposure of a theshold number of shares of the private key, while corruption or loss would mean loss of all shares except a sub-threshold set. In either event a new key would be generated and the subordinate CA public keys re-certified. All subscribers and known relying

parties would be notified as promptly and directly as possible.

### 4.9. CA Termination

When the Fermilab Top-Level CA terminates its services the fact will be advertised, particularly to users and known relying parties. All valid CA certificates will be revoked and the final CRLs will be made widely available, including at the repository location defined in section 2.6.4.

## 5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

### 5.1. Physical Security Controls

The Top-Level CA is operated on hardware which is never connected to any data network and which is stored in locked storage when not in use.

### 5.2. Procedural Controls

The Top-Level CA is not present on any computer except when in use to issue a CA certificate or CRL. Its secret key is shared by the Shamir polynomial method. When the key is needed, shares of the key are loaded with all participating share holders present. All copies of the key or key shares are security erased from the computer before it is returned to storage. In particular, paging space is not used.

### 5.3. Personnel Security Controls

All persons with access to a share of the Top-Level CA's key, will be full-time Fermilab employees in the laboratory directorate or the computer security organization. When any holder of a share of the Top-Level key leaves the Laboratory, or no longer has a computer security role, the secret key shall be reassembled from shares and divided into new shares. The old shares shall all be surrendered and destroyed.

## 6. TECHNICAL SECURITY CONTROLS

### 6.1. Key Pair Generation and Installation

#### 6.1.1. Private Key Generation

The Fermilab Top-Level CA does not generate any private keys but its own. The Top-Level CA key is generated on a system freshly installed from distribution media and then split into shares.

#### 6.1.2. Private Key Delivery to Entity

Not necessary.

#### 6.1.3. Public Key Delivery to Certificate Issuer

Subordinate CA public keys are hand-carried by computer security personnel.

#### 6.1.4. CA Public Key Delivery to Users

The public key of the Top-Level CA is delivered to subscribers and potential relying parties through publication and other unauthenticated channels (except where a secured infrastructure such as PGP or CA cross-certification may already exist) and must be verified through out-of-band means to the satisfaction of relying parties.

#### 6.1.5. Key Sizes

The public RSA modulus of the Fermilab Top-Level CA will be at least 4096 bits in length. All public keys certified by the Fermilab Top-Level CA must have a modulus of at least 2048 bits.

#### 6.1.6. Key Usage

The Fermilab Top-Level CA does not enforce key usage restrictions by any means beyond the X.509v3 extensions in the certificates it issues. CA certificates will have the Key Usage extension set to allow Digital Signature, Certificate Signing, and CRL Signing.

Certificates issued by the Fermilab Top-Level CA are not recommended to be used for non-repudiation, data confidentiality or message integrity.

### 6.2. Private Key Protection

#### 6.2.1. Key Generation Modules

No stipulation.

#### 6.2.2. Multiperson Control

The Top-Level CA's key is held in 3-out-of-7 multiperson control.

#### 6.2.3. Key Escrow

Not Supported.

#### 6.2.4. Private Key Archival and Backup

Not supported, beyond the 3-of-7 redundancy in storage.

#### 6.2.5. CA Private Key Activation

The Top-Level CA key requires the threshold number of shares (three) to be brought together on a system. All holders of participating shares are present for the process and verify the secure erasure of the key after use.

### 6.3. Other Aspects of Key Pair Management

End entity keys are not archived by the Fermilab Top-Level CA. CA keys are not archived beyond their validity period. The Top-Level CA key lifetime is five years.

### 6.4. Activation Data

No stipulation.

### 6.5. Computer Security Controls

The Top-Level CA key is generated on a computer which not connected to any data network during the process, or at any time subsequent. The key is assembled from shares only on that same computer, and securely erased afterward.

### 6.6. Life Cycle Security Controls

No Stipulation

### 6.7. Network Security Controls

The Top-Level CA is never connected to a network, even when the key is not present.

### 6.8. Cryptographic Module Engineering Controls

No Stipulation

## 7. CERTIFICATE AND CRL PROFILES

### 7.1. Certificate Profiles

#### 7.1.1. Subordinate CA Certificates

Subject:
DC=gov/DC=fnal/O=Fermilab/OU=Certificate Authorities/CN=<CA Name>
Issuer:
DC=gov/DC=fnal/O=Fermilab/OU=Certificate Authorities/CN=Top-Level CA
Validity:
( ... )
Subject Public Key Info:
( ... )
X509v3 Extensions:
X509v3 Basic Constraints (critical):
CA:TRUE, pathlen:(generally 0)
X509v3 Authority Key Identifier
keyid:( ... )
X509v3 Subject Key Identifier
( ... )
X509v3 Key Usage: critical
Digital Signature, Certificate Sign, CRL Sign
X509v3 Certificate Policies:
Policy: 1.3.6.1.4.14147.1.5.1.( ... )
CPS: http://computing.fnal.gov/security/docs/( ... )
User Notice:
Organization: Fermilab
Number: ( ... )
Explicit Text: ( ... )
X509v3 CRL Distribution Points:
URI:http://computing.fnal.gov/security/pki/top-level-crl.crl
(Signature ...)

#### 7.1.2. Certificate Policy Object Identifier

iso(1) org(3) dod(6) iana(1) private(4) enterprises(1) Fermilab(14147) security(1) documents(5) topLevel-CPS(1).

### 7.2. CRL Profile

The CRL is in version 1 format.

## 8. Specification Administration

### 8.1. Specification Change Procedures

Peer PKI operators will be notified of changes.

### 8.2. Publication

The policy will be available at http://computing.fnal.gov/security/docs/.

#### 8.2.1. CPS Approval Procedures

The Fermilab computer security team approves practices compliant with this policy and statement.